UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,729	03/22/2004	Phillip Andrew Porras	SRI/3928-9	9573

52197 7590 04/10/2007

PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/805,729	PORRAS ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4-4-06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending in this office action.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-20 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-25 of U.S. Patent No. 6,321,338.

Although the conflicting claims are not identical, they are not patentably distinct from each other because:

Instant application:	Patented Case:
• receiving a plurality of network packets handled by a network entity; • building at least one statistical profile from at least one measure of said plurality of network packets; and • analyzing said at least one statistical profile to detect suspicious network activity.	• receiving network packets handled by a network entity; • building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections; • comparing at least one long-term and at least one short-term statistical profile; and • determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

The patented case compares a short-term profile against a long-term profile to determine suspicious activity, whereas the instant application analyzes at least one profile to determine suspicious activity.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on April 4, 2006, is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner. The remaining IDS's, submitted on October 25, 2004, and April 27, 2006, have not been considered because of the excessive amount of documents listed.

Specification

4. The disclosure is objected to because of the following informalities: paragraph 0001 needs to be updated to include application number 10/254,457, which matured into patent number 6,711,615.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya (U.S. Patent No. 6,279,113).

Regarding claims 1, 19, and 20, Vaidya teaches a method/computer-readable medium/apparatus for performing network surveillance, said method comprising the steps of:

- Receiving a plurality of network packets handled by a network entity (col. 5, lines 26-46);
- Building at least one statistical profile from at least one measure of said plurality of network packets (col. 6, lines 1-11); and
- Analyzing said at least one statistical profile to detect suspicious network activity (col. 6, lines 11-26).

Regarding claim 2, Vaidya teaches wherein said at least one measure monitors data transfers by monitoring network packet data transfer commands (col. 5, lines 33-39, data transport).

Regarding claim 3, Vaidya teaches wherein said at least one measure monitors data transfers by monitoring network packet data transfer errors (col. 5, lines 33-39, unauthorized attempts to access network objects).

Regarding claim 4, Vaidya teaches wherein said at least one measure monitors data transfers by monitoring network packet data transfer volume (col. 5, lines 33-39).

Regarding claim 5, Vaidya teaches wherein said at least one measure monitors network connections by monitoring network connection requests (col. 7, lines 33-36).

Regarding claim 6, Vaidya teaches wherein said at least one measure monitors network connections by monitoring network connection denials (col. 5, lines 33-39, attempted delivery of malicious data packets).

Regarding claim 7, Vaidya teaches wherein said at least one measure monitors network connections by monitoring a correlation of network connection requests and network connection denials (col. 5, lines 33-39 and col. 7, lines 33-36).

Regarding claim 8, Vaidya teaches wherein said at least one measure monitors errors by monitoring at least one error code included in a network packet, wherein said at least one error code comprises a privilege error code or an error code indicating a reason a packet was rejected (col. 5, lines 33-39, unauthorized attempts to access network objects).

Regarding claim 9, Vaidya teaches further comprising the step of responding based on determining whether said at least one statistical profile indicates suspicious network activity (fig. 3, ref. num 66).

Regarding claim 10, Vaidya teaches wherein said responding step comprises transmitting an event record to a network monitor (col. 7, lines 52-67).

Regarding claim 11, Vaidya teaches wherein said transmitting the event record to a network monitor step comprises transmitting the event record to a hierarchically higher network monitor (col. 5, lines 47-51).

Regarding claim 12, Vaidya teaches wherein said transmitting the event record to a network monitor step comprises transmitting the event record to a network monitor that receives event records from a plurality of network monitors (fig. 1, ref. num 12).

Regarding claim 13, Vaidya teaches wherein said network monitor that receives event records from said plurality of network monitors comprises a network monitor that correlates activity in said plurality of network monitors based on said received event records (col. 5, lines 26-46).

Regarding claim 14, Vaidya teaches wherein said responding step comprises altering said analysis of said plurality of network packets (col. 7, lines 31-45).

Regarding claim 15, Vaidya teaches wherein said responding step comprises severing a communication channel (col. 6, lines 21-26).

Regarding claim 16, Vaidya teaches wherein said network entity comprises at least one of a gateway, a router, a proxy server, a firewall, and a virtual private network (VPN) entity (fig. 1, ref. num 20).

Regarding claim 17, Vaidya teaches wherein said plurality of network packets are partitioned into a plurality of sessions representing a communication transaction between two hosts (col. 7, line 52 through col. 8, line 15).

Regarding claim 18, Vaidya teaches wherein said at least one measure monitors network connections by monitoring a source port number and a destination port number included in one of said network packets (col. 2, lines 15-30).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. U.S. Patent No. 6,213,706 (Fan et al.), 5,991,881 (Conklin et al.), and 5,987,610 (Franczek et al.) all disclose intrusion detection systems that analyze network packet signature to determine suspicious activity.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brenda Bernard

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

4/6/07